A

ise type a plus sign (+) inside this box → [+]

r the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

nly for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	1850
First Inventor or Application Identifier	FOX et al.
Title	Certificate Reissuance for Checking the Status of a Certificate in Financial Transactions
Express Mail Label No.	EJ037122585US

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [X] *Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)

2. [X] Specification [Total Pages 45]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. [X] Drawing(s) (35 U.S.C. 113) [Total Sheets 7]

4. Oath or Declaration [Total Pages 2]
a. [X] Newly executed (original or copy)
b. [ ] Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 16 completed)
i. [ ] DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

*NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

5. [ ] Microfiche Computer Program (Appendix)

6. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
a. [ ] Computer Readable Copy
b. [ ] Paper Copy (identical to computer copy)
c. [ ] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. [X] Assignment Papers (cover sheet & document(s))

8. [ ] 37 C.F.R.§3.73(b) Statement (when there is an assignee) [X] Power of Attorney

9. [ ] English Translation Document (if applicable)

10. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations

11. [ ] Preliminary Amendment

12. [X] Return Receipt Postcard (MPEP 503) (Should be specifically itemized)

13. [ ] * Small Entity Statement(s) (PTO/SB/09-12) [ ] Statement filed in prior application, Status still proper and desired

14. [ ] Certified Copy of Priority Document(s) (if foreign priority is claimed)

15. [ ] Other: ....
....
....

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:
[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No: _____/_____

Prior application information: Examiner_____ Group / Art Unit: _____
For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

[ ] Customer Number or Bar Code Label
(Insert Customer No. or Attach bar code label here)
or [X] Correspondence address below

Name	Albert S. Michalik, Reg. No. 37,395
	Michalik & Wylie, PLLC
Address	14645 Bel-Red Road
	Suite 103
City	Bellevue
State	Washington
Zip Code	98007
Country	USA
Telephone	(425) 653-3520
Fax	(425) 653-3603

Name (Print/Type)	Albert S. Michalik	Registration No. (Attorney/Agent)	37,395
Signature	*Albert S. Michalik*	Date	11/23/99

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

In re Application of FOX et al.
Attorney Docket No. 1850

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

"Express Mail" mailing label number EJ037122585US

Date of Deposit: November 23, 1999

I hereby certify that the following documents:

New Patent Application in the name of Barbara L. Fox and Brian A. LaMacchia for "Certificate Reissuance for Checking the Status of a Certificate in Financial Transactions," including 1 Page Cover Sheet, 28 Pages Specification, 15 Pages Claims, 1 Page Abstract, 7 Sheets Of Drawings, Transmittal Sheet, Fee Transmittal Sheet, Executed Declaration and Power of Attorney, Assignment Recordation Cover Sheet and Assignment

are being deposited with the United States Postal Service "Express Mail Post Office To Addressee" Service under 37 C.F.R. 1.10 on the date indicated above and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

Albert S. Michalik
_____
(Typed or printed name of person mailing paper or fee)

_____
(Signature of person mailing paper or fee)

1850 express mail cert

SPECIFICATION

TO ALL WHOM IT MAY CONCERN:

Be it known that we, Barbara L. Fox, a citizen of the United States, residing at 1415 Second Avenue, Seattle, Washington 98101, and Brian A. LaMacchia, a citizen of the United States, residing at 400 Harvard Avenue East, Apt. 201, Seattle, Washington, 98102, have invented a certain new and useful **CERTIFICATE REISSUANCE FOR CHECKING THE STATUS OF A CERTIFICATE IN FINANCIAL TRANSACTIONS** of which the following is a specification.

CERTIFICATE REISSUANCE FOR CHECKING THE STATUS OF A CERTIFICATE IN FINANCIAL TRANSACTIONS

5 ## FIELD OF THE INVENTION

The present invention generally relates to computer systems, and more particularly to transactions performed over a computer-based network such as intranets or the Internet.

10

BACKGROUND OF THE INVENTION

In network transactions, a certificate authority ("CA") is an entity that issues digitally signed certificates ("digital certificates") to other entities such as
15 organizations or individuals to allow them to prove their identity to others in financial or other remote transactions. A certificate authority may be an external company such as one which offers digital certificate services, or may be an internal organization such as a corporate MIS department. The
20 certificate authority's chief function is to ascertain whether a subscriber meets the policy criteria for a class of digital certificates and if so, to issue one. A "subscriber" could be a person, a machine, or an executable.

At present, for financial transactions, online customers
25 obtain a digital certificate from a certificate authority or their bank, and send that digital certificate with a signed transaction request (e.g., purchase order) to a merchant. The

merchant typically verifies the customer's signature using the public key in the certificate and in the process assures that the digital certificate's status is valid (e.g., not revoked). The X.509 standard (ISO/IEC JTC1/SC 21, Draft Amendments DAM 4

5   to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate Extensions, 1 December, 1996) specifies that a way to determine the status of a digital certificate is by using a certificate revocation list ("CRL"). Each certificate authority (or its designated

10   agent) publishes a CRL of digital certificates it has previously issued that are now revoked. The merchant downloads the CRL from the issuing certificate authority and searches the list to make sure that the serial number of the digital certificate in question is not on the list.

15   CRLs cause a variety of problems, one of which is that that the list of all revoked certificates from the certificate authority may potentially become very large. More importantly, a CRL may not be sufficiently current, (i.e. "fresh enough"), whereby reliance thereon creates unacceptable

20   financial risk. This "freshness problem" is particularly dangerous in high-value transactions.

A merchant may also verify a digital certificate by utilizing an Online Certificate Status Checking Protocol ("OCSP"), a presently proposed standard by which the

certificate authority or a verification company makes an independent assertion about a digital certificate's validity. With OCSP like other insurance schemes, financial risk is purposely assumed by the certificate authority or verification

5 company in exchange for a per-transaction fee. The certificate authority or verification company determines if the digital certificate is revoked, and returns a good, revoked or unknown status.

While OCSP is thus potentially more up-to-date than CRL-

10 based solutions, OCSP has a number of economically-motivated peculiarities and limitations that make it less than ideal for many transactions. For example, an OCSP response is essentially an up-to-date one-certificate CRL, returning only either the good, revoked or unknown assertion about a

15 certificate in an entirely new message format. Moreover, OCSP presumes a particular risk management pricing model that attaches a high cost and high liability to the issuance of every certificate status assertion. As such, OCSP depends upon its own three-tier (Client-Certificate Authority-

20 Designated Responder) infrastructure, wherein the number of qualified certificate issuers and designated status responders is highly limited. In typical financial transactions, however, acceptance policy is up to the policy of the party buying the risk, and there is no reason to limit the parties

to transactions to the narrow OCSP model, let alone to the simplistic certificate status assertion of good, revoked or unknown.

<div style="text-align:center">SUMMARY OF THE INVENTION</div>

The present invention is directed to a method and system for using a certificate authority to first provide a customer with a digital certificate, and then having a relying third party who receives that digital certificate from the customer access a status authority (the certificate authority or a designated agent of the certificate authority) to receive a second, reissued digital certificate on the first digital certificate or its public key. The reissued digital certificate has a relatively much shorter validity period than the first certificate, which relies on a certificate's expiring before its assertion could become false. The length of the validity period is determined by an associated risk management equation which includes, for example, the dollar amount of the transaction and the credit-worthiness of the customer.

Moreover, the reissued digital certificate serves as a receipt including an accumulated record of the signatures (digital certificates) and possibly other accumulated evidence throughout the financial transaction. As a result, the

- 4 -

receipts generated on each transfer of a transaction adds to the digital chain of evidence, recording each step of the transaction and policy applied thereto, whereby risk may be assumed and charged for appropriately. The present invention

5   is accomplished by simple extensions to existing protocols, i.e., without requiring new overly complex protocols and data structures, and further can return detailed information with each response.

Other advantages will become apparent from the following

10   detailed description when taken in conjunction with the drawings, in which:

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a block diagram representing a computer

15   system into which the present invention may be incorporated;

FIG. 2 is a block diagram representing a general architecture for performing a financial or other transaction over a network in accordance with one aspect of the present invention;

20   FIG. 3 is a block diagram representing a financial transaction performed in accordance with one aspect of the present invention;

FIG. 4 is a block diagram representing a data structure of selected various fields of a reissue certificate formed in accordance with one aspect of the present invention;

FIG. 5 is a block diagram representing a financial transaction performed in accordance with an aspect of the present invention;

FIG. 6 is a block diagram representing a series of financial transactions performed in accordance with one aspect of the present invention; and

FIG. 7 is a flow diagram generally representing the steps for issuing a reissue digital certificate upon an existing digital certificate in accordance with one aspect of the present invention.

DETAILED DESCRIPTION

Exemplary Operating Environment

FIGURE 1 and the following discussion are intended to provide a brief general description of a suitable computing environment in which the invention may be implemented. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by a personal computer. Generally, program modules include routines, programs,

objects, components, data structures and the like that perform
particular tasks or implement particular abstract data types.

Moreover, those skilled in the art will appreciate that
the invention may be practiced with other computer system

5   configurations, including hand-held devices, multi-processor
systems, microprocessor-based or programmable consumer
electronics, network PCs, minicomputers, mainframe computers
and the like. The invention may also be practiced in
distributed computing environments where tasks are performed

10 by remote processing devices that are linked through a
communications network. In a distributed computing
environment, program modules may be located in both local and
remote memory storage devices.

With reference to FIG. 1, an exemplary system for

15 implementing the invention includes a general purpose
computing device in the form of a conventional personal
computer 20 or the like, including a processing unit 21, a
system memory 22, and a system bus 23 that couples various
system components including the system memory to the

20 processing unit 21. The system bus 23 may be any of several
types of bus structures including a memory bus or memory
controller, a peripheral bus, and a local bus using any of a
variety of bus architectures. The system memory includes
read-only memory (ROM) 24 and random access memory (RAM) 25.

- 7 -

A basic input/output system 26 (BIOS), containing the basic routines that help to transfer information between elements within the personal computer 20, such as during start-up, is stored in ROM 24. The personal computer 20 may further

5   include a hard disk drive 27 for reading from and writing to a hard disk, not shown, a magnetic disk drive 28 for reading from or writing to a removable magnetic disk 29, and an optical disk drive 30 for reading from or writing to a removable optical disk 31 such as a CD-ROM or other optical

10   media. The hard disk drive 27, magnetic disk drive 28, and optical disk drive 30 are connected to the system bus 23 by a hard disk drive interface 32, a magnetic disk drive interface 33, and an optical drive interface 34, respectively. The drives and their associated computer-readable media provide

15   non-volatile storage of computer readable instructions, data structures, program modules and other data for the personal computer 20. Although the exemplary environment described herein employs a hard disk, a removable magnetic disk 29 and a removable optical disk 31, it should be appreciated by those

20   skilled in the art that other types of computer readable media which can store data that is accessible by a computer, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, random access memories (RAMs), read-only

memories (ROMs) and the like may also be used in the exemplary operating environment.

A number of program modules may be stored on the hard disk, magnetic disk 29, optical disk 31, ROM 24 or RAM 25,

5   including an operating system 35, (including a file system therein and/or associated therewith), one or more application programs 36, other program modules 37 and program data 38. A user may enter commands and information into the personal computer 20 through input devices such as a keyboard 40 and

10   pointing device 42. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner or the like. These and other input devices are often connected to the processing unit 21 through a serial port interface 46 that is coupled to the system bus, but may be

15   connected by other interfaces, such as a parallel port, game port or universal serial bus (USB). A monitor 47 or other type of display device is also connected to the system bus 23 via an interface, such as a video adapter 48. In addition to the monitor 47, personal computers typically include other

20   peripheral output devices (not shown), such as speakers and printers.

The personal computer 20 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 49. The remote computer

49 may be another personal computer, a server, a router, a

network PC, a peer device or other common network node, and

typically includes many or all of the elements described above

relative to the personal computer 20, although only a memory

5   storage device 50 has been illustrated in FIG. 1. The logical

connections depicted in FIG. 1 include a local area network

(LAN) 51 and a wide area network (WAN) 52. Such networking

environments are commonplace in offices, enterprise-wide

computer networks, intranets and the Internet.

10   When used in a LAN networking environment, the personal

computer 20 is connected to the local network 51 through a

network interface or adapter 53. When used in a WAN

networking environment, the personal computer 20 typically

includes a modem 54 or other means for establishing

15   communications over the wide area network 52, such as the

Internet. The modem 54, which may be internal or external, is

connected to the system bus 23 via the serial port interface

46. In a networked environment, program modules depicted

relative to the personal computer 20, or portions thereof, may

20   be stored in the remote memory storage device. It will be

appreciated that the network connections shown are exemplary

and other means of establishing a communications link between

the computers may be used.

Online Certificate Status Checking in Financial Transactions

While the present invention was originally implemented in a financial environment and thus includes financial-based client and server examples, it should be understood that the present invention is not limited to financial applications, but instead has numerous applications throughout user computing. Moreover, although the various components are shown and described herein as separate components because of certain benefits resulting from separated functionality, it can be readily appreciated that some or all of the components may be combined into more complex components, and/or separated even further into additional components.

FIG. 2 shows a representation of a general architecture for performing a financial or other transaction over a network, such as the Internet, in accordance with the present invention. In the example shown, an online customer sends a request to a merchant to enter a particular transaction. The online customer in this example is an "end entity" 60 (the seller of the financial transaction), and the merchant is the "relying party" 62 (the buyer of the financial transaction).

In general, the present invention is directed to method and system by which the relying party 62 authenticates the end entity 60 so that a transaction can be entered. Initially, before the transaction can occur, the end entity 60 obtains a

digital certificate 64 from a certificate authority 66 ("CA"),

as represented in FIG. 2 by the arrows labeled with circled

numerals one and two, respectively. More particularly, to

request the original digital certificate 64, the end entity 60

5   generates a private key 67 and a public key 68 (or uses a pair

previously generated) and submits a certification request to

the certificate authority 66. This is represented in FIG. 2

by the arrow labeled with circled numeral one. The

certificate authority 66 determines via a policy manager 69 if

10   the request satisfies the certificate authority's certificate

issuance policy and, if so, the certificate authority 66

processes the request by creating a digitally-signed statement

including the public key 68 of the end-entity 60 and identity

information about the end-entity 60. The resulting

15   certificate 64 is a statement by the certificate authority 66

attesting to the binding between the identity information, and

possession of both the private key 67 and the public key 68.

The certificate authority 66 uses a digital signature

scheme (e.g., public key cryptography) to create a binding

20   among some identity information, e.g., the end entity's

possession of the private key 67 and the public key 68. The

digital certificate 64 comprises a digitally-signed statement

about the public / private key pair 68, 67, and is returned to

the end entity 60 (the arrow numbered two in FIG. 2). The

digital certificate 64 is signed using the certificate

authority's private key 70 and can be verified by anyone

holding a copy of the certificate authority's public key 71.

All communications involve only the public key, and the

5   private key is never transmitted or shared. While the present

invention is described with reference to public key

cryptography, it is understood that the features of the

present invention may be utilized with any digital signature

scheme or the like. The end entity 60 may use its private key

10   67 to electronically sign a transaction, and include the

digital certificate 64 as evidence of its own identity i.e.,

authenticate that the end entity 60 is qualified to enter the

transaction.

As shown in FIGS. 2 and 3, to initiate a transaction, the

15   end entity 60 sends (transmits as shown by the arrow labeled

three) a transaction request 72 to the relying party 62 (e.g.,

merchant) along with the digital certificate 64 (FIG. 3). The

digital certificate 64 and the transaction request 72 are

received by the relying party's external interface 74 (FIG.

20   2), and are forwarded to a policy evaluation engine 76. The

relying party's policy evaluation engine 76 makes a policy

decision to determine whether the submitted evidence

comprising the digital certificate 64 and possibly other

information satisfies its own acceptance policy for the

- 13 -

transaction. For transactions deemed "high-value" according

to the relying party's policy, the relying party's policy

evaluation engine 76 requires real-time proof that the end

entity's public key 68 and / or the digital certificate 64

5   have not been revoked or otherwise compromised. Other

information may be used and/or required by the policy

evaluation engine 76, as described below.

In accordance with the present invention and as is

described below, after receiving the digital certificate 64,

10   to obtain real-time status information on the certificate 64,

the relying party 62 accesses a status authority (i.e., the

certificate authority 66 or a designated agent thereof) to

receive a second, "reissued" digital certificate on the

digital certificate 64. To request real-time status

15   information regarding the digital certificate 64, the relying

party's policy evaluation engine 76 requests, via a request

message 77 (and the arrow labeled four in FIGS. 2 and 3), a

status inquiry from the certificate authority 66. The request

message 77 may seek the status of the digital certificate 64,

20   and / or the status of the underlying public key 68.

As shown in FIG. 2, the certificate authority 66 receives

the request at an external interface 78. Although the status

request message 77 is depicted in FIG. 3 as being sent

directly to the issuing certificate authority 66 as the status

- 14 -

authority, in practice the request may be directed to an agent

authorized to emit status information on behalf of the issuing

certificate authority. The certificate authority 66 shown in

the drawings thus also represents the status authority,

5   including any such agent, although not separately shown for

purposes of simplicity.

The request message 77 may comprise the digital

certificate 64, and / or any other prior issued digital

certificate or certificates that were submitted by the end

10   entity 60 to the relying party 62. For example, if the

relying party wants current information regarding the status

of the digital certificate 64, the message delivered to the

responder may be exactly the digital certificate 64.

The digital certificate 64 may also be submitted to the

15   certificate authority 66 as the request message 77 for

information regarding the status of the public key 68. Some

additional information may be added to the digital

certificate 64 (e.g., header information) to indicate that a

response about the public key 68 is desired, and not a

20   response about the digital certificate 64 carrying the public

key.

The public key 68 may also be extracted from the digital

certificate 64, and forwarded to the certificate authority as

the request message 77 for real-time status of the public key.

However, if such a method is used, the request message may need to be distinguished from a request for an original certificate.

The request message 77 may take a variety of different formats, including the formats and protocols of existing industry standards. Slight variations may be required to use some of the existing protocols. For example, the *de facto* industry standard for requesting a digital certificate for a public / private key pair is defined by a protocol known as the PKCS#10 protocol. PKCS#10 messages are self-signed to provide proof-of-possession of the corresponding private key. In the case of real-time status checking, the requesting party (i.e., the relying party 62) is not normally the same entity as that possessing the key pair in question, and thus does not possess the private key. Thus, if PKCS#10 message format is to be used, the certificate authority 66 is altered so as to receive a public key, an existing digital certificate, or both of these items with additional information. For example, the request could be slightly altered so as to distinguish the request from a standard PKCS#10 message by adding header information or the like identifying the request as a real-time status inquiry of an existing digital certificate or public key.

The request message 77 could also utilize the existing

extensibility in the proposed CMS (Cryptographic Message

Syntax)-based certificate enrollment protocol known as CMC.

In CMC, the Full Enrollment Request message is a signed CMS

5   with commands (zero or more) and enrollment requests (zero or

more). The certificates to be checked could be included the

CertificateSet portion of a SignedData CMS content payload.

That is, the body of the CMS SignedData message becomes simply

a data structure of the form:

10

```
SEQUENCE OF
  SEQUENCE {
    id-realtime-status-request      // an OBJECT IDENTIFIER
    requestSubject                  // a ResponseSubject
15  }
  }
```

where ResponseSubject is an extension that is added to a

digital certificate to create a reissue certificate (described

20   below), and the request for the ResponseSubject, as indicated

by "requestSubject", is an indication that a reissue

certificate is requested. The ResponseSubject request

provides a reference either to a particular public / private

key pair (by referencing the key identifier of a public key),

25   or to a particular certificate, either by a hash of the

certificate or by an (issuer name, serial number) pair. The

type of request being made, i.e., public key versus

certificate, is implicit in the choice of identifier.

- 17 -

In response to the request message 77, the status
authority (e.g., the certificate authority 66 via the policy
manager 69) issues a "reissue" digital certificate 80 (FIG.
3), attesting to the current validity of the subject

5   certificate. The reissue digital certificate 80 is distinct
from the certificate 64, and can be provided in a variety of
formats, but preferably is provided in the existing X.509v3
protocol format. By using an existing standard as opposed to
creating a new message type, existing public key

10   infrastructure ("PKI") clients and certificate servers require
only minimal modifications to take advantage of the present
invention.

An example of the differences between selected various
fields of the reissue certificate 80 and the certificate 64

15   are shown in FIG. 4. As can be seen, the reissue digital
certificate 80 takes much of the same form as the original
certificate, and includes the same Issuer Name and Subject
Name. The reissue digital certificate 80 includes an Issuer
Serial Number, different than the Serial Number of the

20   original digital certificate 64, that uniquely identifies the
reissue digital certificate 80. The validity period of the
reissue digital certificate 80 is narrowed to the window in
which the reissue digital certificate is valid. This period
may be set to a desired age, and is likely to be significantly

- 18 -

shorter than the validity period of the original digital
certificate 64 and, for many transactions, may be less than
one day in duration.

In a preferred embodiment, the certificate authority adds

5   to the original digital certificate 64 a new extension 82
indicating that it is a freshness assertion about a public key
or a digital certificate. The presence of the extension 82
(which is identified by its own "object identifier" (OID)) can
serve as notice that the reissue certificate 80 is a response

10 to a status check. The data contained in the extension 82,
called *ResponseSubject* in the example shown in FIG. 4,
references the object for which status was requested: a public
key or a certificate. One way to do this is to use a modified
form of the AuthorityKeyIdentifier data type defined in Public

15 Key Infrastructure Exchange (PKIX) Part 1, Section 4.2.1.1:

```
    ResponseSubject ::= SEQUENCE {
        keyIdentifier       [0] KeyIdentifier              OPTIONAL,
        certIdentifier      [1] CertIdentifier             OPTIONAL,
        certIssuer          [2] GeneralNames               OPTIONAL,
20      certSerialNumber    [3] CertificateSerialNumber    OPTIONAL,
    }

    KeyIdentifier ::= OCTET STRING

25  CertIdentifier ::= SEQUENCE {
        hashAlgorithm           AlgorithmIdentifier,
        certHash                CertHash
    }

30  CertHash ::= OCTET STRING
```

As can be seen in the above example, a ResponseSubject extension 82 may include a reference to a particular public key (denoted by keyIdentifier), a reference to a particular digital certificate via hash (certIdentifier), and / or a

5   reference to an issuer / serial-number pair (certIssuer, certSerialNumber). Since the keyIdentifier is presumed to correspond to a SubjectKeyIdentifier contained within the digital certificate 64, there is no need to identify a hash algorithm for it. For the CertIdentifier structure, a

10   certificate hash (algorithm and hash function output) is needed to uniquely identify the digital certificate that is the subject of the response.

In the case of a failure, i.e., rejection, the certificate authority 66 may fail to return a response,

15   although this is not particularly desirable or useful to the relying party 62. Alternatively, the certificate authority 66 may return some other signed statement including information concerning why the status check failed. Another possibility is to add another extension 84 (called "ResponseStatus" in

20   FIG. 4) to the reissue digital certificate 80 that explicitly contains success / failure information. The relying party's policy evaluation engine 76 could check such explicit information as part of its evaluation of the reissue digital certificate 80.

The certificate authority 66 may choose to add other

extensions to the reissue digital certificate 80 as evidence

that its policy has been met. For example, an Evidence List

extension 84 could be added that contains information

5   regarding the evidence submitted to satisfy the policy of the

relying party 62. Additionally, a Certificate Policy

extension 86 could be added that includes policy-related

information that semantically qualifies the response.

Additional extensions could be added to provide desired

10   information with the reissue digital certificate 80.

The reissue certificate 80 is forwarded to the relying

party's policy evaluation engine 76, and is combined with the

transaction request 72, the digital certificate 64 and any

other submitted evidence to make a determination if the

15   information meets the relying party's trust management

question. The policy evaluation may include only the above-

described real-time status check on the submitted certificate

or the underlying public key (FIG. 3), but may further

additional local inquiries, such as an application-specific

20   real-time check (e.g., communication with a bank to determine

current credit-worthiness), and / or an evaluation of locally-

held policy-related information, such as the relying party's

prior transaction history with this particular end entity 60.

FIG. 5 shows a financial transaction in which additional

local inquiries, other than the status of a public key and /

or a digital certificate, may be required by the policy

evaluation engine 76.   The additional policy information may

5   be requested in the request message 77 and evaluated by the

certificate authority 66, or may be determined independent of

the certificate authority.   If determined by the certificate

authority 66, the information is added to the reissue

certificate 80.   If determined by the relying party, digitally

10   signed signatures 87 or the like regarding the locally

determined policy information may be generated and combined

with the reissue digital certificate 80 or, alternatively, the

relying party may issue another reissue certificate

incorporating the new information.

15   Following the policy evaluation, the relying party's

policy evaluation engine 76 generates an acceptance or denial

result, and a statement of the decision is returned to the end

entity 60, along with the digital reissue certificate 80 and

digitally signed signatures 87, if any.   This is shown in

20   FIGS. 2, 3 and 5 by the arrow labeled with circled numeral

six.   In the case of acceptance, the reissue digital

certificate 80 and local policy digital signatures 87, (if

any), are forwarded to the end entity 60 as a receipt 88 (FIG.

5). The end entity 60 is thus supplied with information regarding the policy applied to the transaction.

After issuing the receipt 88, the relying party 62 may wish to re-sell the transaction to a third party. The buyer in the previous transaction (the relying party 62) then becomes the seller of the transaction, and the previously-issued receipt is now a piece of evidence submitted to the new buyer proving that the old buyer (i.e., the relying party 62) applied its own policy at the time it purchased the transaction. The new buyer of the transaction may then request a new reissue certificate and produce a new receipt, and can sell the transaction to a new party, and so on.

For example, FIG. 6 illustrates how accumulated signed receipts, generated as part of the process of selling and re-selling a single transaction, encapsulate the transaction's history. Initially, party A holds transaction T and receipt / certificate $Cert_1$, which describes how party A came to hold the transaction. Party A proposes to sell the transaction T to party B and sends party B the transaction T along with the receipt / certificate $Cert_1$ and other supporting evidence, if necessary. Party B evaluates the evidence to see that it satisfies its policy and if so, issues a receipt / certificate ("$Cert_2$") as proof that its policy was satisfied. The new receipt / certificate $Cert_2$ is returned to party A and the

- 23 -

transaction between party A and party B concludes. Party B

now holds transaction T, receipt / certificate $Cert_1$ (which

references T) and receipt / certificate $Cert_2$ (which references

both transaction T and $Cert_1$).

5   Party B may then re-sell the transaction T to party C.

As above, party B first sends the transaction T to the

proposed buyer along with supporting evidence. The evidence

submitted by B will ordinarily include both the evidence

submitted by party A to party B when party B bought the

10   transaction T, as well as the receipt / certificate $Cert_2$ that

party B issued showing that party B's acceptance policy was

satisfied. Party C performs its own acceptance policy

evaluation and issues receipt / certificate $Cert_3$ as proof of

acceptance of the transaction. This new receipt / certificate

15     $Cert_3$, which references the transaction T and

receipt/certificates $Cert_1$ and $Cert_2$, is returned to party B to

complete the resale of the transaction. A further resale in a

similar manner of the transaction T from party C to party D is

shown in FIG 6, resulting in party D issuing a receipt /

20   certificate $Cert_4$.

At the conclusion of the three sales of the

transaction T, party D holds the transaction T and four

receipt / certificates — $Cert_1$, $Cert_2$, $Cert_3$ and $Cert_4$.

Together, these receipt / certificates detail exactly how

- 24 -

transaction T moved among the four parties, what policy

decisions were made along the way, and the commitments made by

each party in the process. Even after the transaction

terminates and no longer exists, the receipts persist and

5   continue to provide evidence. For example, should the

transaction T be repudiated at a later date, the signed

receipt / certificates may be used to prove or refute a claim.

Thus, the set of receipts/certificates generated by every

transfer of the transaction forms a digitally-signed chain of

10   evidence binding not only every step of the transaction but

also every policy application that happened along the way. Of

course, it is feasible to include less information than the

total accumulated with each additional transaction.

Turning now to an explanation of the operation of the

15   present invention, FIG. 7 shows a general overview of a

process for issuing a reissue certificate in accordance with

one aspect of the present invention. Beginning at step 700,

the end entity 60 ("EE"), already possessing a digital

certificate 64 ("Cert.") from the certificate authority 66,

20   forwards the digital certificate, along with a transaction

request 72, to the relying party 62 ("RP"). The relying

party 62 requests real-time status information regarding the

end entity 60 (step 702).

As described above, the real-time status inquiry may be regarding the status of the digital certificate 64, or the status of the underlying public key 68 for the digital certificate. If information regarding the status of the

5   public key 68 is desired, step 704 branches to step 706, where the relying party 62 sends information identifying the public key ("PK") to the status authority (e.g., the certificate authority 66). As also described above, this information may be, for example, the extracted public key 68, the digital

10   certificate 64 with additional information indicating that a status request regarding the public key is desired, or a command requesting the public key information by hash. At step 708, the certificate authority 66 issues a reissue certificate on the public key 68.

15   Alternatively, if information regarding the digital certificate 64 is desired, step 704 branches to step 710 where the relying party 62 sends information identifying the digital certificate 64 to the status authority (e.g., the certificate authority 66). As described above, this information may

20   include, for example, the digital certificate 64, the issuer name and serial number for the digital certificate, or other sufficient information to identify the digital certificate 64. The certificate authority 66 issues a reissue certificate

(e.g., the reissue certificate 80) on the digital certificate 64.

At step 714, a determination is made, for example by the relying party's policy evaluation engine 76, as to whether the relying party's policy is met. As described above, this inquiry may include only the real-time status check of the digital certificate 64, or may additionally include local inquiries regarding the transaction or the end entity 60. If the relying party's policy is not met, step 714 branches to step 716 where the reissue certificate ("RC") and a message informing the end entity 60 of the rejection of the requested transaction is forwarded to the end entity.

If, however, the relying party's policy is met, step 714 branches to step 718 where the reissue certificate 80 and relying party policy information are combined to form a receipt. The receipt is forwarded to the end entity 60 in step 720.

As can be seen from the above detailed description, there is provided a system and method for certificate re-issuance to validate a transaction. The system and method may be accomplished via extensions to existing protocols, and further allow receipts including policy information to be generated with each transaction. The present invention may be implemented independent of the underlying form of public key

infrastructure, and without reliance on a limited number of qualified certificate issuers and designated status responders. With the present invention, response to a real-time status check is a risk transference just like certificate

5   issuance.

While the invention is susceptible to various modifications and alternative constructions, a certain illustrated embodiment thereof is shown in the drawings and has been described above in detail. It should be understood,

10   however, that there is no intention to limit the invention to the specific form or forms disclosed, but on the contrary, the intention is to cover all modifications, alternative constructions, and equivalents falling within the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1.   A computer-readable medium having computer-executable instructions, comprising:

receiving a first transaction request in association with

5   a first certificate issued by a certificate authority;

communicating with a status authority to query for

current status information on the first certificate; and

receiving a second certificate from the status authority

indicating the current status of the first certificate.

10

2.   The computer-readable medium of claim 1, wherein the

certificate authority comprises the status authority.

3.   The computer-readable medium of claim 1, wherein the

15   status authority comprises an agent authorized to act on

behalf of the certificate authority.

4.   The computer-readable medium of claim 1, wherein the

transaction request is received from an end entity, and having

20   further computer executable instructions comprising,

transmitting information including the second certificate to

the end entity.

5.   The computer-readable medium of claim 4, wherein the information including the second certificate is transmitted to the end entity along with a response to the transaction request.

5

6.   The computer-readable medium of claim 4, wherein the information including the second certificate is transmitted to the end entity along with at least one digital signature.

10   7.   The computer-readable medium of claim 1 having further computer executable instructions comprising, transmitting the first certificate and the second certificate to a remote party along with a second transaction request.

15   8.   The computer-readable medium of claim 7 having further computer executable instructions comprising, receiving a third certificate from the remote party.

9.   The computer-readable medium of claim 8, wherein
20 information of the third certificate is communicated with a response to the second transaction.

10.   The computer-readable medium of claim 1, wherein a third certificate is received with the transaction request and

the first certificate, the third certificate comprising a record of a response to a status request of the first certificate at a particular time.

5   11.   The computer-readable medium of claim 10 having further computer executable instructions comprising, transmitting the first certificate, the second certificate, and the third certificate to a remote party along with another transaction request.

10

       12.   The computer-readable medium of claim 11 having further computer executable instructions comprising, receiving information including a fourth certificate from the remote party indicating the current status of at least one of the

15   first, second, and third certificates.

       13.   The computer-readable medium of claim 11, wherein the fourth certificate is communicated with a response to the other transaction.

20

       14.   A computer-readable medium having computer-executable instructions, comprising:

       receiving a query from a relying party for current status information on a first certificate; and

issuing a data structure including a second certificate indicating the current status of the first certificate.

15. The computer-readable medium of claim 14, having further computer executable instructions comprising transmitting the data structure to the relying party.

16. The computer-readable medium of claim 14, wherein the data structure comprises an extension designating the second certificate as being an indication of the current status of the first certificate.

17. The computer-readable medium of claim 14, wherein the data structure further comprises policy information.

18. The computer-readable medium of claim 17, wherein the data structure further includes information regarding evidence submitted to satisfy a policy of the relying party.

19. The computer-readable medium of claim 14, wherein the data structure comprises policy-related information that qualifies the second certificate.

20. The computer-readable medium of claim 14, wherein the data structure further comprises success or failure information regarding the second certificate.

5   21. The computer-readable medium of claim 14, wherein the data structure comprises information regarding a validity period of the second certificate.

         22. The computer-readable medium of claim 21, wherein
10 the first certificate has a validity period associated therewith, and wherein the information regarding the validity period of the second certificate specifies a validity period for the second certificate that is shorter than the validity period for the first certificate.

15

         23. A method for performing electronic commerce, comprising,

         receiving, at a certificate authority, a first request for a certificate;

20   verifying whether the certificate should be issued, and if so, issuing the certificate;

         receiving a second request at a status authority for status information about the certificate; and

issuing a reissue certificate including the status information.

24. The method of claim 23 wherein the certificate authority comprises the status authority.

25. The method of claim 23 wherein the status authority is a designated agent of the certificate authority.

26. The method of claim 23 wherein the first request is provided by an end entity.

27. The method of claim 23 wherein the second request is provided by a relying party.

28. The method of claim 23 wherein the first request is provided by an end entity that provides the certificate to a relying party, and wherein the second request is provided by the relying party.

29. A method for performing electronic commerce, comprising:

receiving a certificate at an end entity;

providing the certificate to a relying party; and

receiving a receipt at the end entity from the relying party, the receipt including status information about the certificate.

5   30.   The method of claim 29 further comprising, requesting the certificate from a certificate authority.

31.   The method of claim 29 wherein the status information is provided by a status authority.

10

32.   The method of claim 29 further comprising, requesting a certificate from a certificate authority, and wherein the status information is provided by the certificate authority.

15

33.   The method of claim 29 wherein the receipt includes evidence.

34.   The method of claim 33 wherein the evidence
20   comprises policy information.

35.   A method for performing electronic commerce, comprising,

receiving a certificate with a request to perform a transaction;

communicating with a status authority to request status information about the certificate;

5   receiving a reissue certificate including the status information in response to the request; and

deciding whether to perform the transaction based on the status information.

10   36. The method of claim 35 wherein the certificate is issued by a certificate authority.

37. The method of claim 35 wherein the certificate authority further comprises the status authority such that the

15   certificate and reissue certificate are issued by the certificate authority.

38. The method of claim 35 wherein the request to perform a transaction is received from an end entity, and

20   further comprising returning a response to the end entity.

39. The method of claim 35 wherein the response includes a receipt.

40.   The method of claim 35 wherein the receipt includes data associated with the status information.

41.   The method of claim 35 wherein the certificate is issued by a certificate authority, and wherein the request to perform a transaction is received from an end entity, and further comprising returning a response to the end entity.

42.   A method for performing electronic commerce, comprising:

requesting at an end entity a certificate from a certificate authority;

providing the certificate with a request for performance of a transaction; and

receiving information at the end entity indicating whether the transaction was performed, the information provided by a status authority and including the status of the certificate.

43.   The method of claim 42 wherein the certificate authority comprises the status authority.

44.   The method of claim 42 wherein the information received at the end entity includes a receipt.

45.   A method for performing electronic commerce,
comprising:

requesting at an end entity a certificate from a

5   certificate authority;

providing a request for performance of a transaction to a
relying party, the request including the certificate;

receiving the request at the relying party, and
communicating with a status authority to determine the status

10   of the certificate;

receiving a reissue certificate from the status
authority, the reissue certificate indicating the status of
the certificate; and

communicating information from the relying party to the

15   end entity, the information indicating whether the transaction
was performed and including the status of the certificate.

46.   A method for performing electronic commerce,
comprising:

20   receiving, at a second party, a request from a first
party to accept a transaction and a first certificate
referencing the transaction;

accepting the transaction at the second party and issuing a receipt to the first party, the receipt including a second certificate as proof of acceptance of the transaction;

sending, from the second party to a third party, the

5   transaction, the first certificate and the second certificate to offer the transaction for sale; and

receiving a receipt at the second party from the third party including a third certificate as proof that the third party purchased the transaction.

10

47.   The method of claim 46 wherein the third party sends the transaction, the first certificate, the second certificate and the third certificate to a fourth party to attempt to resell the transaction.

15

48.   The method of claim 46 wherein the fourth party purchases the transaction and issues a receipt including a fourth certificate to the third party.

20   48.   The method of claim 46 wherein the first certificate comprises evidence, and wherein the second party evaluates the evidence from the first party.

49.   The method of claim 48 wherein the evidence includes at least one policy decision made by the first party.

50.   The method of claim 46 wherein the first and second certificates comprise evidence, and wherein the third party evaluates the evidence from the first party and the second party.

51.   The method of claim 50 wherein the evidence includes at least one policy decision made by at least one of the first or second parties.

52.   The method of claim 46 wherein the first, second and third certificates comprise evidence, and wherein the fourth party evaluates the evidence from the first party, the second party and the third party.

53.   The method of claim 50 wherein the evidence includes at least one policy decision made by at least one of the first, second or third parties.

54.   The method of claim 46 wherein each party evaluates each certificate provided thereto prior to issuing its respective receipt.

- 40 -

55. A computer-readable medium having stored thereon a data structure, comprising:

a first field referencing a request for performing an electronic transaction; and

a second field comprising a list of evidence accumulated from at least one recipient of the request.

56. The computer-readable medium having stored thereon the data structure of claim 55, wherein the first field comprises a response subject field.

57. The computer-readable medium having stored thereon the data structure of claim 55 further comprising, a third field having response status information therein.

58. The computer-readable medium having stored thereon the data structure of claim 55 further comprising, a third field having response status information therein.

59. The computer-readable medium having stored thereon the data structure of claim 55 further comprising, a third field having a validity period identified therein.

60. The computer-readable medium having stored thereon the data structure of claim 55 further comprising, a third field having certificate policy information therein.

5   61. The computer-readable medium having stored thereon the data structure of claim 55 further comprising, a third field having certificate policy information therein.

62. A computer-readable medium having stored thereon a
10 data structure, comprising,

a first data field representing the current status of a first certificate; and

a second data field designating the present data structure as including status information regarding the first
15 certificate.

63. The computer-readable medium of claim 62, wherein the data structure further comprises a third data field providing an evidence list.

20

64. The computer-readable medium of claim 62, wherein the data structure further comprises information regarding evidence submitted to satisfy a policy of the remote recipient.

65. The computer-readable medium of claim 62, wherein the data structure comprises policy-related information.

5   66. The computer-readable medium of claim 62, wherein the current status field indicates success or failure information.

67. The computer-readable medium of claim 62, wherein
10   the data structure comprises information regarding a validity period.

ABSTRACT

A system for using a certificate authority to first provide a customer with a digital certificate, and then having a relying party that receives that digital certificate access a status authority (the certificate authority or its designated agent) to receive a reissued certificate on that certificate. The reissued certificate has a much shorter validity period, which ensures that the information is timely. Moreover, the certificate may serve as a receipt, including an accumulated record of the signatures (digital certificates) and policy applied throughout the financial transaction. As a result, each transfer of the transaction forms a digitally-signed chain of evidence recording each step of the transaction and policy applied thereto, whereby risk may be assumed and charged for appropriately and in accordance with the risk purchaser's policy.
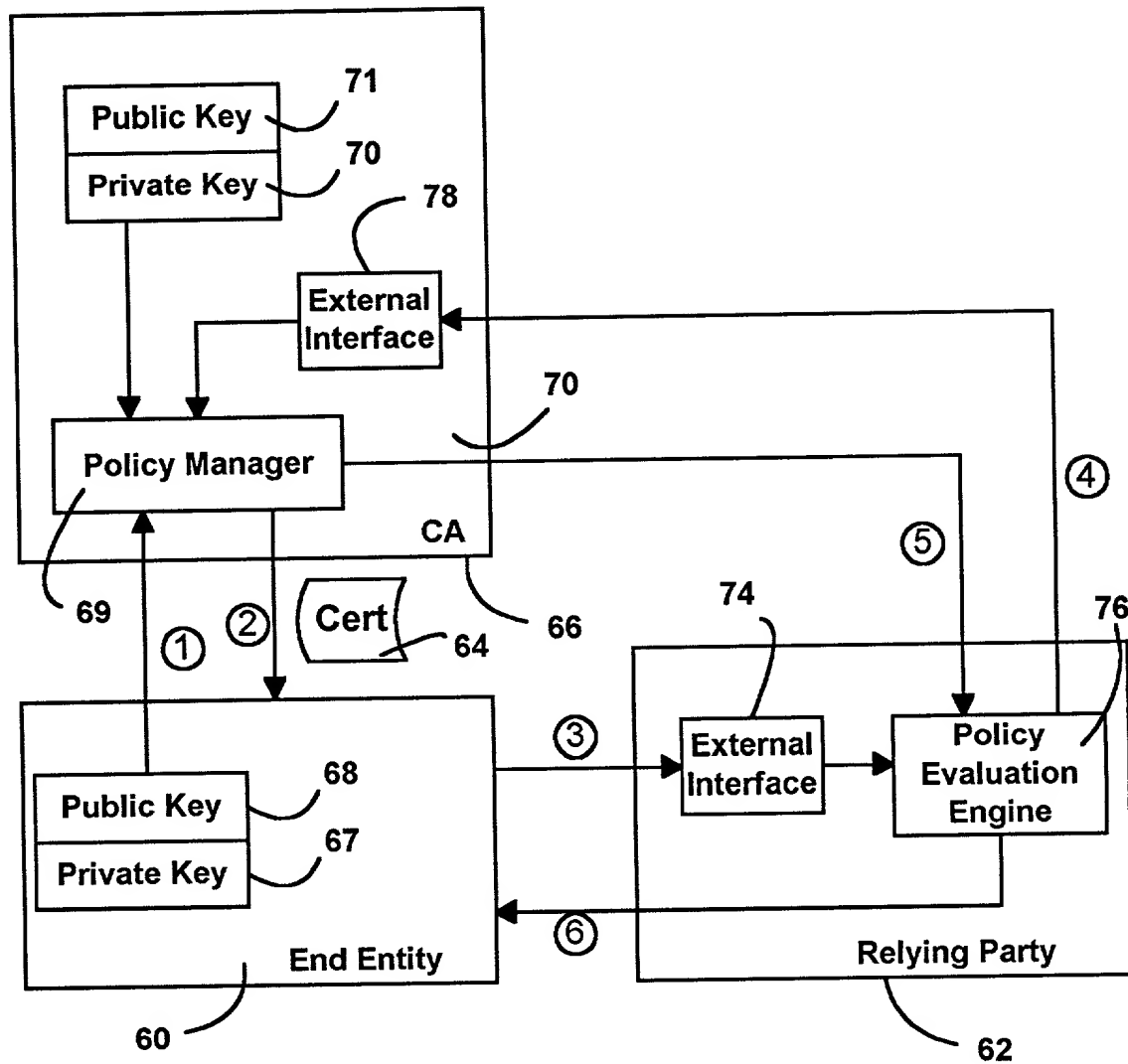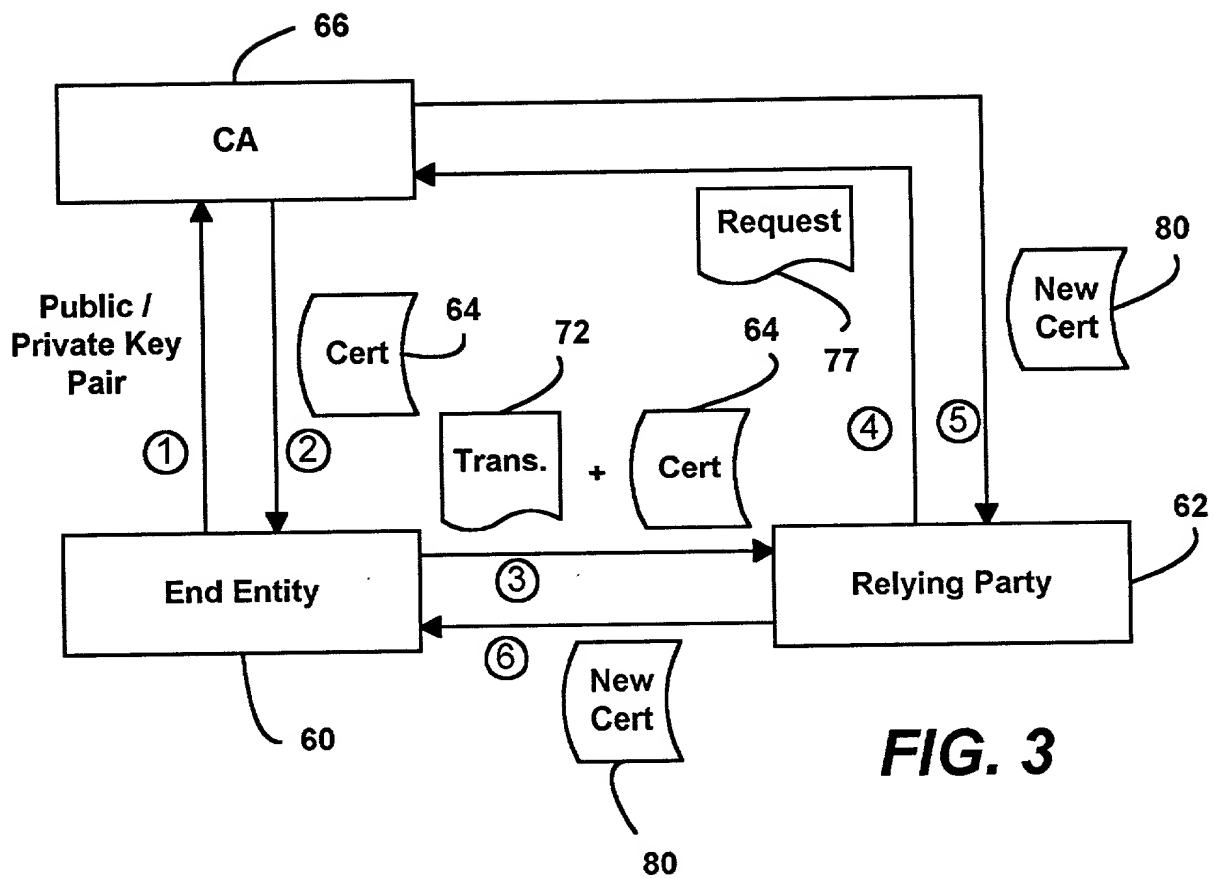
FIG. 1

System Memory
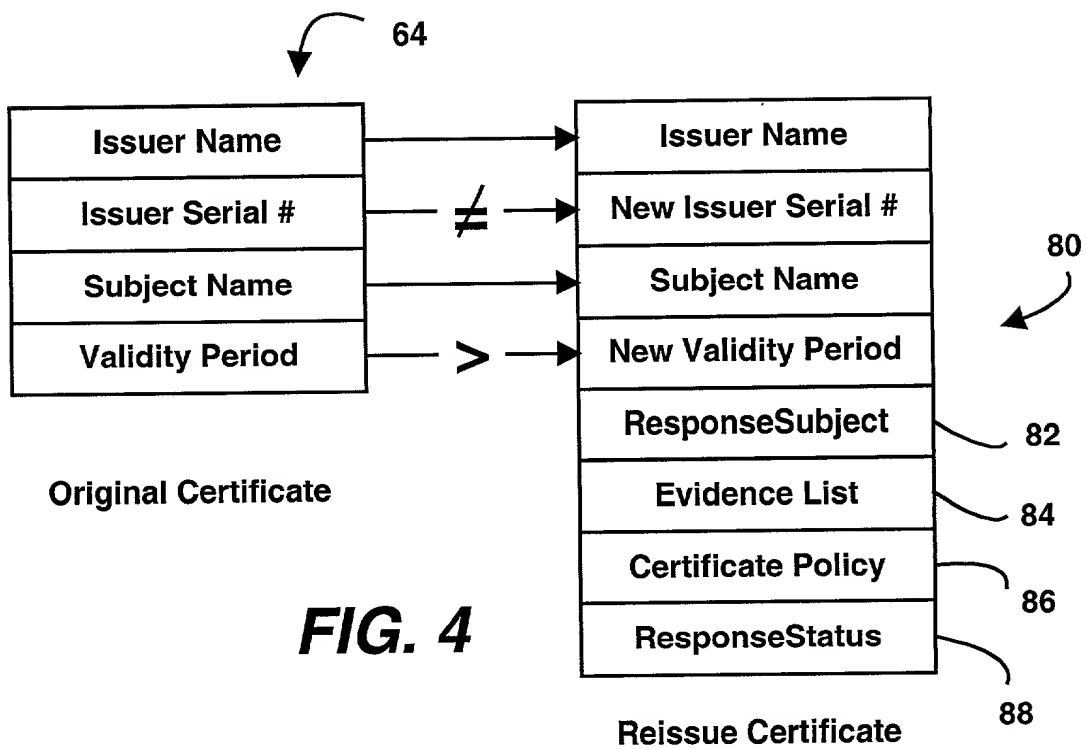
(ROM) **24**

BIOS **26**

(RAM) **25**

OPERATING SYSTEM **35** (with file system)

APPLICATION PROGRAMS **36**

OTHER PROGRAM MODULES **37**

PROGRAM DATA **38**

20

Processing Unit **21**

22

23

System Bus

Video Adapter **48**

Hard Disk Drive Interface **32**

Magnetic Disk Drive Interface **33**

Optical Drive Interface **34**

Serial Port Interface **46**

Network Interface **53**

27

28

29

30

31

OP SYS **35** (with file system)	APPLICATION PROGRAMS **36**	OTHER **37** PROGRAM MODULES	PROGRAM DATA **38**

Monitor **47**

Mouse **42**

Keyboard **40**

Modem **54**

Local Area Network

Wide Area Network **52**

Remote Computer **49**

51

50

APPLICATION PROGRAMS **36'**

FIG. 2

FIG. 3

Original Certificate

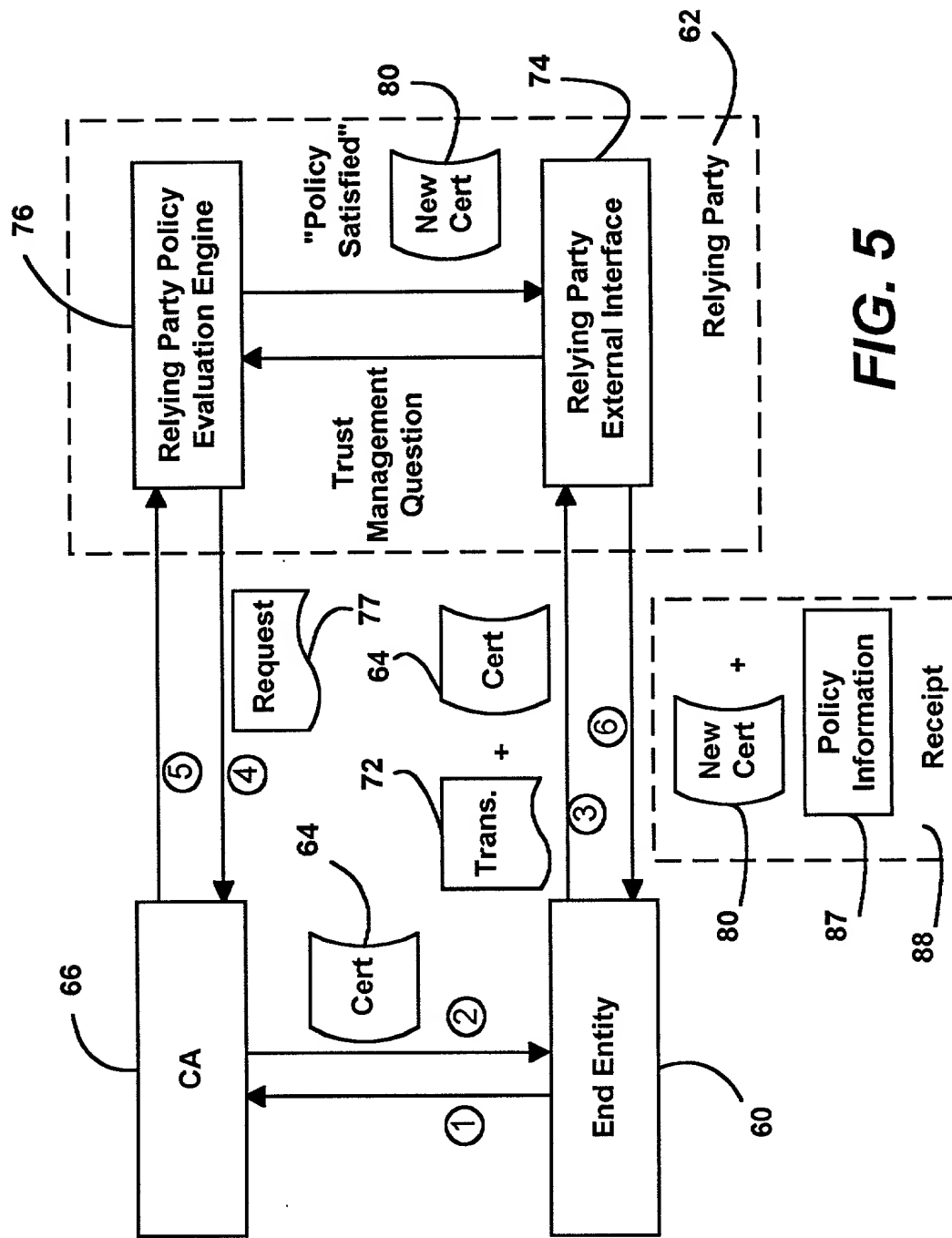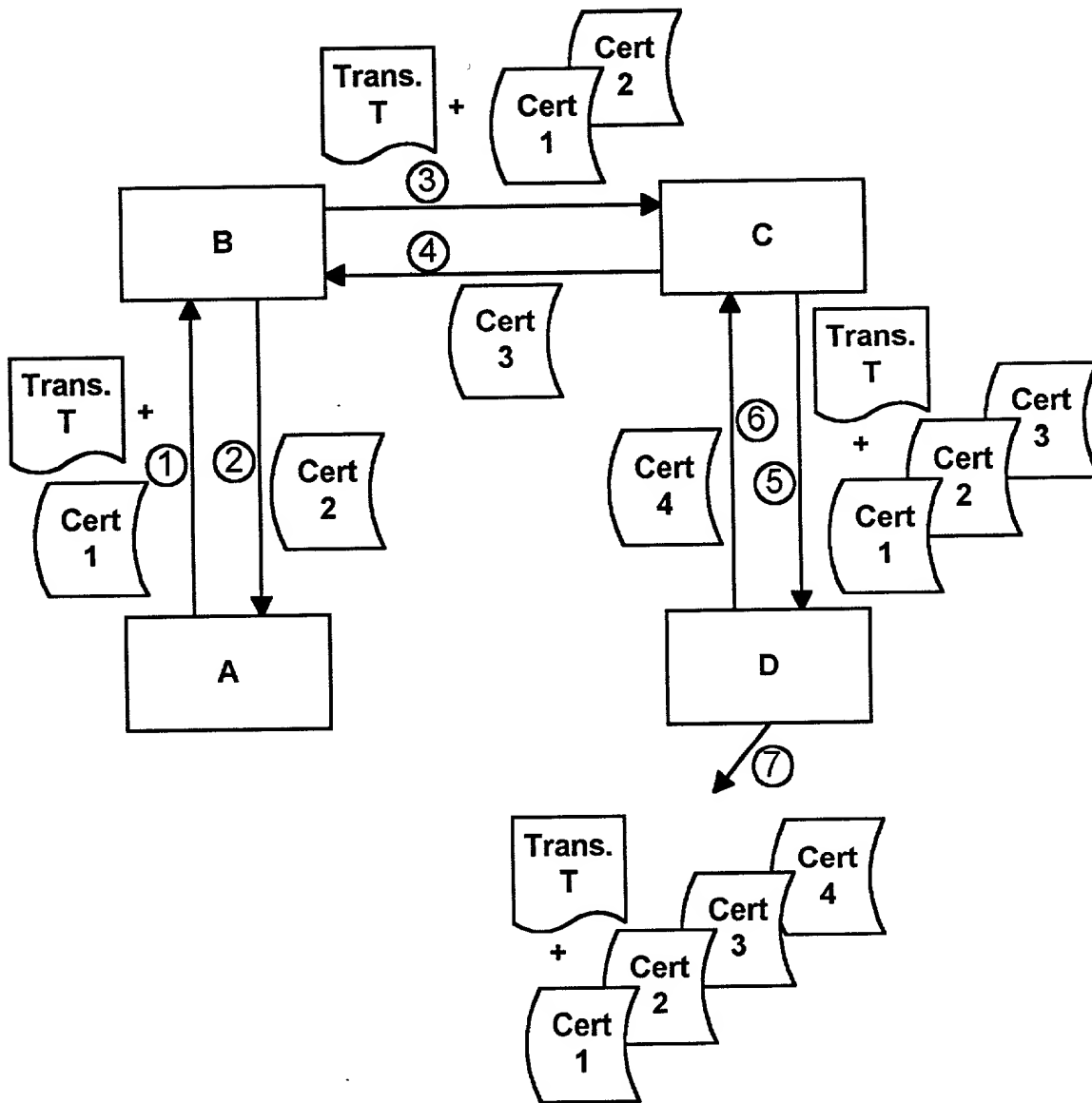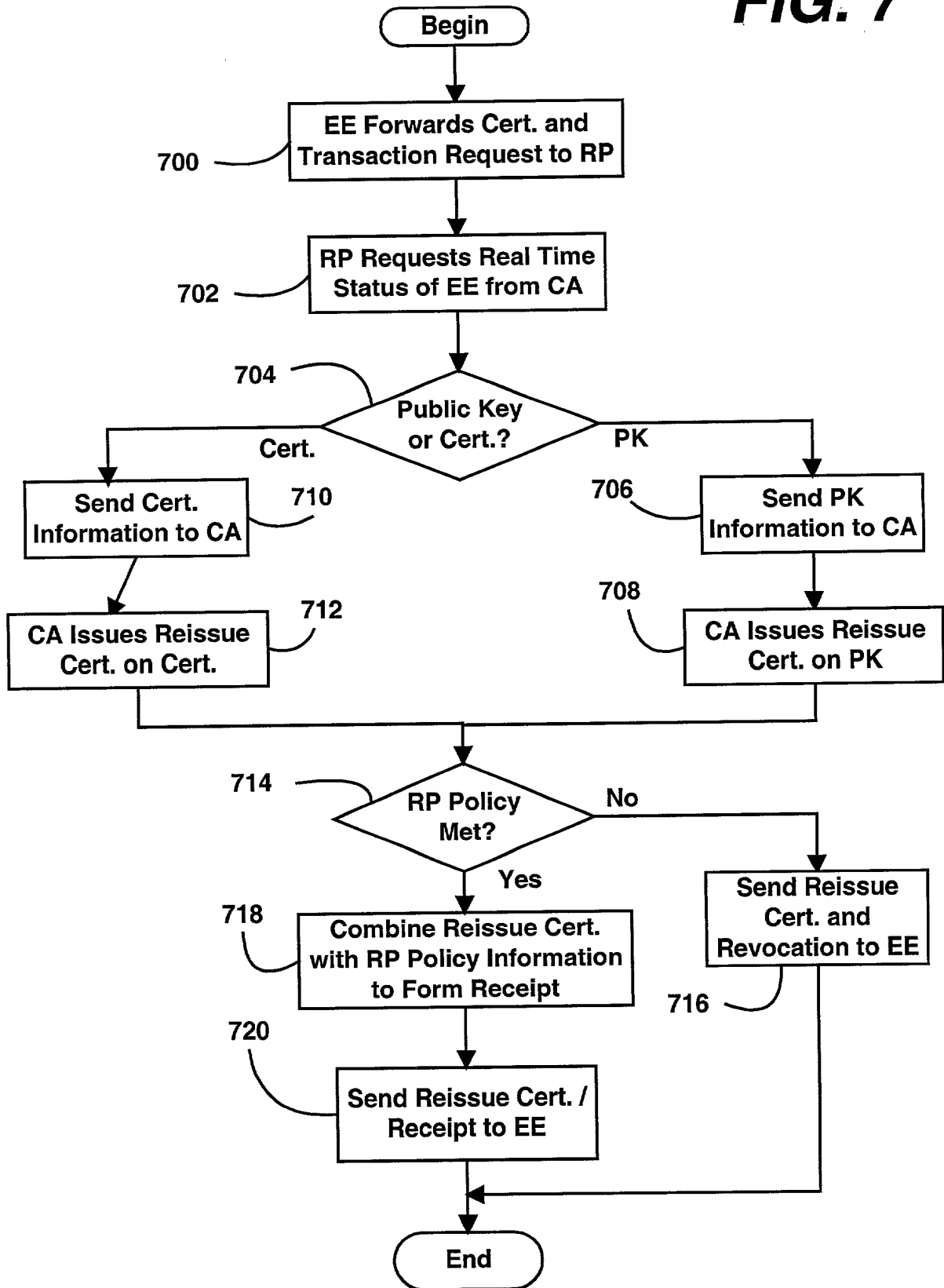**FIG. 4**

Reissue Certificate

FIG. 5

FIG. 6

FIG. 7

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: "Certificate Reissuance for Checking the Status of a Certificate in Financial Transactions," the specification of which is attached hereto unless the following box is checked:

☐   was filed on   as United States Application Serial No.   or PCT International Application No. _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F.R. § 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)   Priority Not Claimed

(Number)	(Country)	(Day/Month/Year Filed)	☐
(Number)	(Country)	(Day/Month/Year Filed)	☐

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below.

(Application Number)	(Filing Date)
(Application Number)	(Filing Date)

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or § 365(c) of any PCT international application(s) designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application(s) in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F.R. § 1.56 which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application.

(Application Number)	(Filing Date)	(Status – patented, pending, abandoned)
(Application Number)	(Filing Date)	(Status – patented, pending, abandoned)

1

As a named inventor, I hereby appoint the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Albert S. Michalik, Reg. No. 37,395 Daniel D. Crouse, Reg. No. 32,022
Roger D. Wylie, Reg. No. 36,794   Katie E. Sako, Reg. No. 32,628
John E. Whitaker, Reg. No. 42,222

Address all telephone calls to   Albert S. Michalik at telephone number (425) 653-3520.

Address all correspondence to: Michalik & Wylie, PLLC
                                         14645 Bel-Red Road
                                         Suite 103
                                         Bellevue, WA 98007

I hereby declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of **sole or first inventor**: Barbara L. Fox

Inventor's signature _____

Date _____11/23/99_____   Country of Citizenship: USA

Residence: 1415 Second Avenue, Seattle, Washington 98101

Post Office Address: Same

Full name of **second joint inventor**, if any: Brian A. LaMacchia

Inventor's signature _____

Date _____11/18/99_____   Country of Citizenship: USA

Residence: 400 Harvard Avenue E, Apt. 201, Seattle, Washington 98102

Post Office Address: 14150 NE 20th Street, No. 246, Bellevue, Washington 98007

☐   Additional inventors are being named on separately numbered sheets attached hereto.

1850 declaration

2